Doc Code: AP.PRE.REQ

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
A-8919 (191930-1960)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]	Application Number	Filed
	10/602,987	June 25, 2003

on _____

Signature_____

	First Named Inventor
	Wasileswski, et al.

Typed or printed name _____	Art Unit	Examiner
	2131	Chai, Longbit

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
      Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☐ attorney or agent of record.
Registration number _____

☒ attorney or agent acting under 37 CFR 1.34.

    48,472

Registration number if acting under 37 CFR 1.34 _____

/Karen G. Hazzah/
Signature

Karen G. Hazzah
Typed or printed name

770-933-9500
Telephone number

07/15/08
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:
    Wasilewski, et al.

Serial No.:
    10/602,987

Filed:
    June 25, 2003

For:
    Method for Partially Encrypting Program Data

Group Art Unit:
    2131

Examiner:
    Chai, Longbit

Docket No.:
    A-8919 (191930-1960)

REMARKS IN SUPPORT OF
PRE-APPEAL BRIEF CONFERENCE

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

    Applicant submits the following remarks in support of a Request for a Pre-Appeal Brief Conference.

REMARKS

    Applicant respectfully submits that the Examiner's rejections of the claims in the pending application are clearly in error. In the outstanding Office Action (mailed April 15, 2008, Paper No. 20080328), the Examiner alleges that since packets in a video stream have different service types, and these packets are encrypted, this implies that packets are selected for encryption based on the service type. This is clear error, since under this rationale, <u>all</u> the components could be encrypted instead.

I.   <u>Rejection of Claims 1-19 under 35 U.S.C. §103</u>

    Claims 1-19 have been rejected under §103(a) as allegedly obvious over U.S. (5,418,782 to *Wasilewski* (hereinafter *Wasilewski* '782) in view of U.S. 5,081,678 to *Kaufman*

(hereinafter *Kaufman*). Although Applicant believes independent claims 1 and 13 are patentably distinct, the clear errors in rejecting similar elements for these claims are presented together here to facilitate review. Furthermore, since independent claims 1 and 13 are allowable, claims 2-12 and 14-19 are allowable for at least the reason that each depends from an allowable claim.

A. Independent Claims 1 and 13

1. The Office Action Allegation

The Office Action (p. 5) contends that the proposed combination *Wasilewski* '782 and *Kaufman* teaches "using a packet identifier to select for encryption a portion of each of a plurality of digital bit streams from a transport stream", using the following reasoning. First, the Office Action asserts that *Wasilewski* '782 teaches ():

> (a) the packets of a data stream can be partially encrypted based on the service type of the packet such as video, audio or data (V/A/D) service type - i.e., to select for encryption a portion of each of a plurality of digital bit stream from a transport stream (i.e. partially encrypted from a video, audio or data (V/A/D) combined data stream) (Wasilewski: Column 4 Line 58 - 67) and (b) the packet ID (PID) is available to identify a packet as one of video, audio or data (VIAID) service types (Wasilewski: Column 14 Line 4 - 7 and Column 13 Line 57 - 59: each type of audio, video and data elementary streams is uniquely assigned a packet ID (PID)).
> (Office Action, p. 4, emphasis in original)

Next, the Office Action (p. 4, emphasis in original) admits that "*Wasilewski* '782 does not disclose explicitly using the packet ID to select which packets to be encrypted," but further contends that *Kaufman* teaches:

> using a packet ID for encryption can provide the advantage for simplifying the decryption task at the receiver by using packet ID as an indicator of the encryption / decryption key (Kaufman: Column 2 Line 12-17 / Line 2-10 / Line 44-56: the key identifier placed inside a transported packet can be considered as one type of packet identifier).
> (Office Action, p. 4, emphasis in original).

2. Cited Portion of *Wasilewski* '782

The Office Action allegations that are disputed by Applicant rely on a small portion of *Wasilewski* '782, reproduced below:

Each basic service comprises a set of related service components, such as video (V), audio (A) and closed-captioning (CC) service components, as shown. In the present embodiment, the service components comprise digital data, however, the present invention is not limited thereto and may also be employed in systems that transmit analog service components or a combination of digital and analog service components. Moreover, one or more service components of a given basic service may be compressed and/or encrypted prior to transmission.
(*Wasilewski* '782, Col. 4, lines 58-67.)

3.   Cited Portion of *Kaufman*

The Office Action allegations that are disputed by Applicant rely on a small portion of

Kaufman, reproduced below:

Each data packet contains sufficient information for the receiving node to ascertain which key to use to decrypt and/or check the integrity of a data packet. This information may either be implicit, i.e., based upon the source address information, or explicit, i.e., based upon a key identifier placed in the packet.
(*Kaufman*, Col. 2, lines 2-10.)

Also, the receiving node in performing the look up operation in its key table does this to find the sending node's key so that it can use that key to decrypt or check the integrity of the data…A common method used to facilitate the look up operation is to have the two nodes exchange an index in the data packet. This index serves as an index into the receiving node's look up table. The index enables the receiving node to locate the sending node's key, thus, enabling the receiving node to decrypt and/or check the received data.
(*Kaufman*, Col. 2, lines 44-56.)

4.   Refutation of the Office Action Allegation

        a. *Wasilewski* '782 does not teach "encryption based on service type"

The Office Action alleges that the above portion of *Wasilewski* '782 teaches partial

encryption "based on service type of the packet". Applicant first notes that this quoted language

does not appear in claim 1 or claim 13. However, the Examiner uses this alleged teaching in

Wasilewski '782 (encryption based on service type) with *Kaufman*'s alleged teaching of using a

packet ID for encryption, to combine into the features recited in claims 1 and 13. Therefore,

Applicant will address the Examiner's characterization of *Wasilewski* '782.

Wasilewski '782 does not teach any mechanism for selecting packets for encryption,

based on anything. The single paragraph in *Wasilewski* '782 relied upon by the Office Action

3

simply states that components can be encrypted. Although *Wasilewski* '782 teaches that components are identified by a PID (program identifier), this does not imply that the PID is used to select particular components for encryption, because <u>all</u> the components could be encrypted instead. Thus, the Examiner's characterization of *Wasilewski* '782 is clear error.

b. *Kaufman* does not teach a "packet identifier"

The Office Action states that *Kaufman* teaches "using packet ID as an indicator of the encryption/decryption key", and then draws the conclusion that "the key identifier placed inside the transported packet can be considered as one type of <u>packet identifier</u>" (Office Action, p. 4, emphasis in original). Applicant submits that the conclusion does not follow from this premise, and that the plain meaning of "key identifier" is something that identifies a key rather than a packet. Thus, the Examiner's characterization of *Kaufman* is clear error.

c. <u>The combination of *Wasilewski* '782 and *Kaufman* does not teach the claimed features</u>

The Office Action characterizes *Wasilewski* '782 as teaching "selecting packets for encryption based on X" and then uses *Kaufman* to replace X with a "packet identifier" – with the alleged result being Applicant's claimed features. As discussed above, *Wasilewski* '782 is deficient because it does not teach X – it does not teach any criteria used to select packets for encryption. Since the primary reference does not teach that which is relied on, the combination is deficient in teaching the claimed features.

As also discussed above, the key identifier in *Kaufman* does not properly correspond to the "packet identifier" recited in claim 1. Applicant will nonetheless now assume, for the sake of argument, that a key identifier in *Kaufman* properly corresponds to a "packet identifier".

Applicant submits that a person of ordinary skill in the art would not be motivated to use the key identifier in *Kaufman* **to select packets for encryption**. The key identifier in *Kaufman* is used to convey encryption information to the receiver without putting the key itself in the packet. Specifically, and as shown above, *Kaufman* teaches that the key identifier is an index into a key table which is commonly shared by transmitter and receiver. *Kaufman* does not deal with the

4

problem of selecting packets for encryption, but instead deals with the problem of how to convey

encryption information once the packets are selected and encrypted. Therefore, a person of

ordinary skill in the art would not look to *Kaufman*'s teachings about conveying encryption

information in order to select packets for encryption. Thus, the Examiner's proposed

combination of *Wasilewski* '782 and *Kaufman* is clear error.

Accordingly, the proposed combination of *Wasilewski* '782 in view of *Kaufman* does not

teach at least the features described above and recited in claims 1 and 13. Therefore, a *prima*

facie case establishing an obviousness rejection has not been made, and the rejection should

be withdrawn.

CONCLUSION

Applicant respectfully requests that all outstanding objections and rejections be

withdrawn and that this application and presently pending claims 1-19 be allowed to issue.

Respectfully submitted,

By: /Karen G. Hazzah/

Karen G. Hazzah, Reg. No. 48,472

THOMAS, KAYDEN, HORSTEMEYER
    & RISLEY, L.L.P.

600 Galleria Parkway, NW
Suite 1500
Atlanta, Georgia 30339-5948
Tel: (770) 933-9500
Fax: (770) 951-0933